US 20020012446A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0012446 A1

Tanaka (43) Pub. Date: Jan. 31, 2002

(54) ELECTRONIC WATERMARK INSERTION DEVICE, DETECTION DEVICE, AND METHOD

(76) Inventor: Nobuyuki Tanaka, Tokyo (JP)

Correspondence Address:
McGuireWoods
1750 Tysons Boulevard, Suite 1800
McLean, VA 22102-4215 (US)

(21) Appl. No.: 09/895,217

(22) Filed: Jul. 2, 2001

(30) Foreign Application Priority Data

Jul. 5, 2000 (JP) 204080/2000

Publication Classification

(51) Int. Cl.[7] G06K 9/00; G06K 9/36; G06K 9/46

(52) U.S. Cl. 382/100; 382/250

(57) ABSTRACT

The use of the undefined low-order four bits of an 8-bit watermark is defined and, when contents are reproduced, a predetermined operation is performed according to the information stored in the low-order four bits. That is, a watermark is added to an original image to create an image with the watermark inserted. When the contents are reproduced, the watermark is detected in the image and, based on the information stored in the low-order four bits of the detected watermark, a predetermined operation, for example, access to a web site on the Internet, is performed.

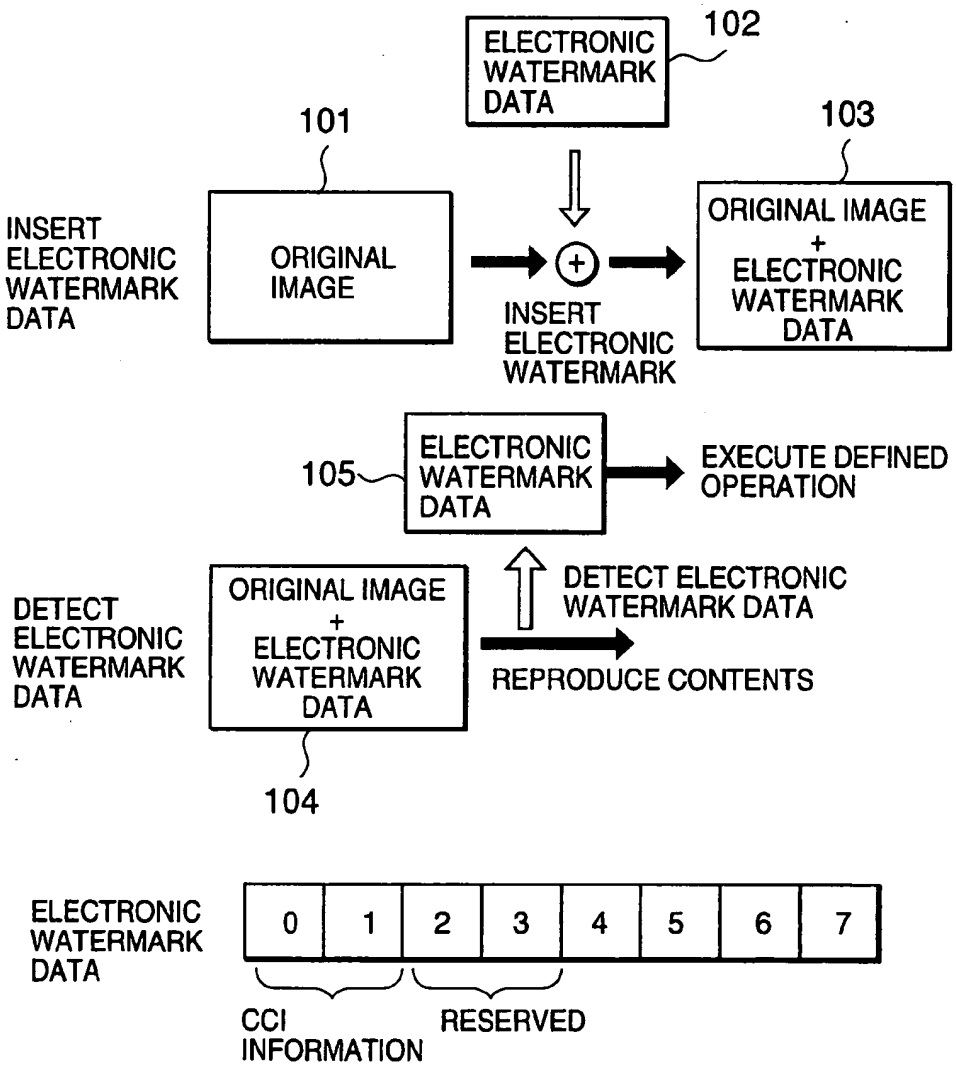
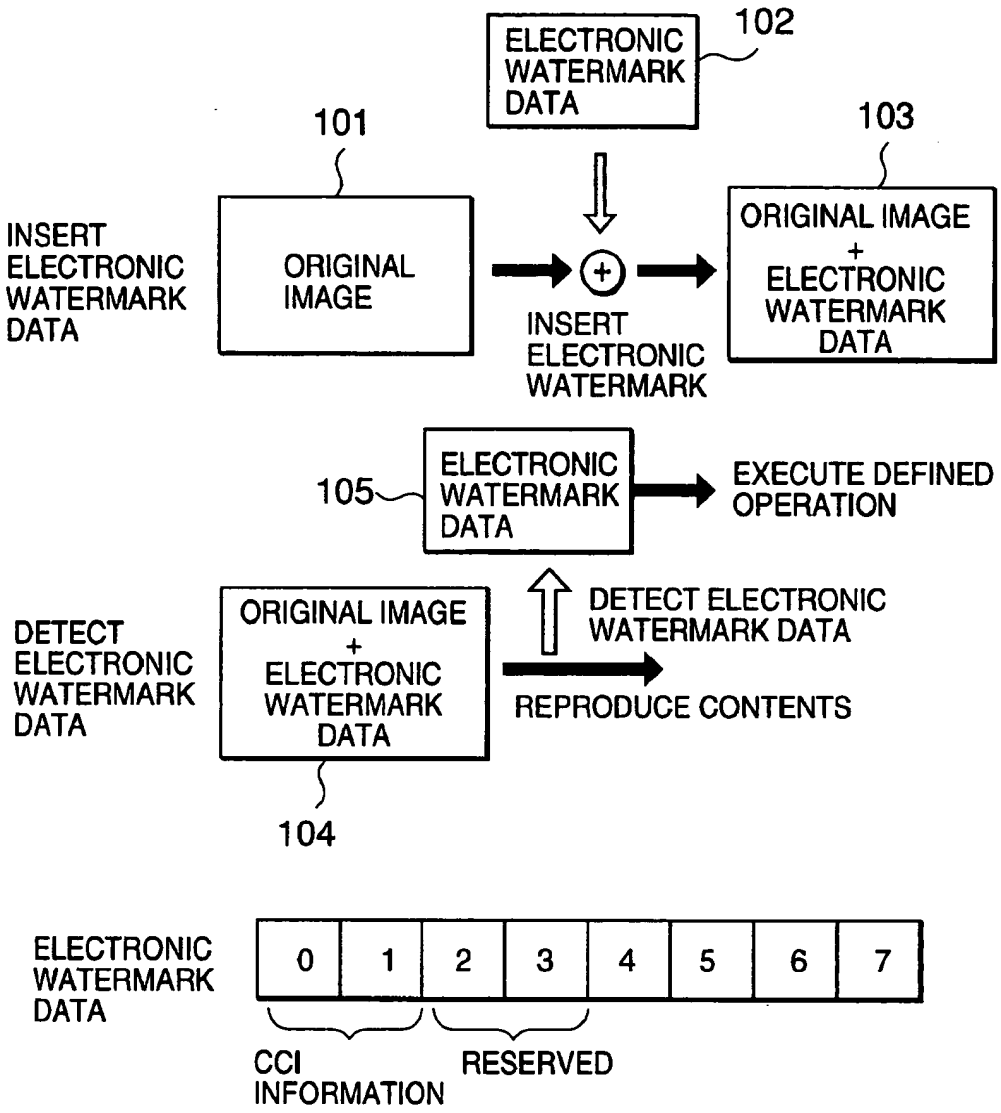


FIG.1


ELECTRONIC WATERMARK DATA
102
101
103
INSERT ELECTRONIC WATERMARK DATA
ORIGINAL IMAGE
ORIGINAL IMAGE + ELECTRONIC WATERMARK DATA
INSERT ELECTRONIC WATERMARK
105
ELECTRONIC WATERMARK DATA
EXECUTE DEFINED OPERATION
DETECT ELECTRONIC WATERMARK DATA
DETECT ELECTRONIC WATERMARK DATA
ORIGINAL IMAGE + ELECTRONIC WATERMARK DATA
REPRODUCE CONTENTS
104
ELECTRONIC WATERMARK DATA
0
1
2
3
4
5
6
7
CCI INFORMATION
RESERVED

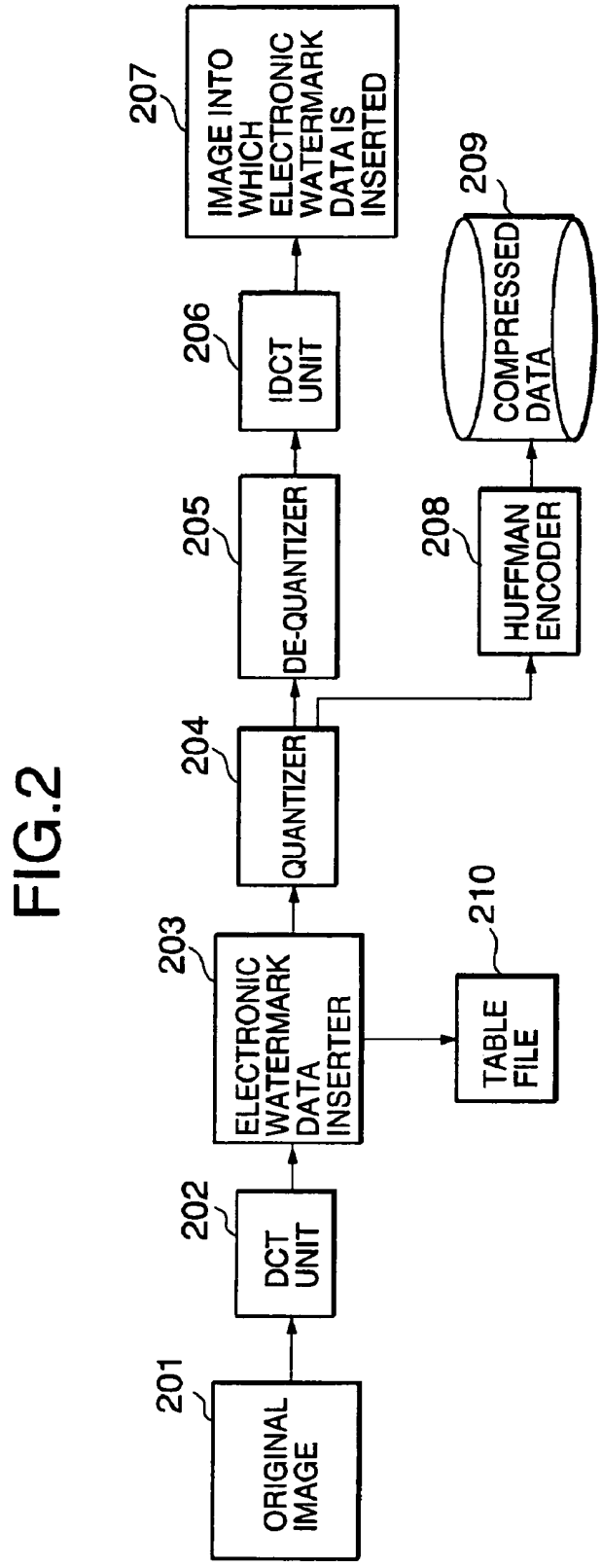

ORIGINAL IMAGE
201
DCT UNIT
202
ELECTRONIC WATERMARK DATA INSERTER
203
TABLE FILE
210
QUANTIZER
204
DE-QUANTIZER
205
IDCT UNIT
206
IMAGE INTO WHICH ELECTRONIC WATERMARK DATA IS INSERTED
207
HUFFMAN ENCODER
208
COMPRESSED DATA
209

FIG.2

FIG.3

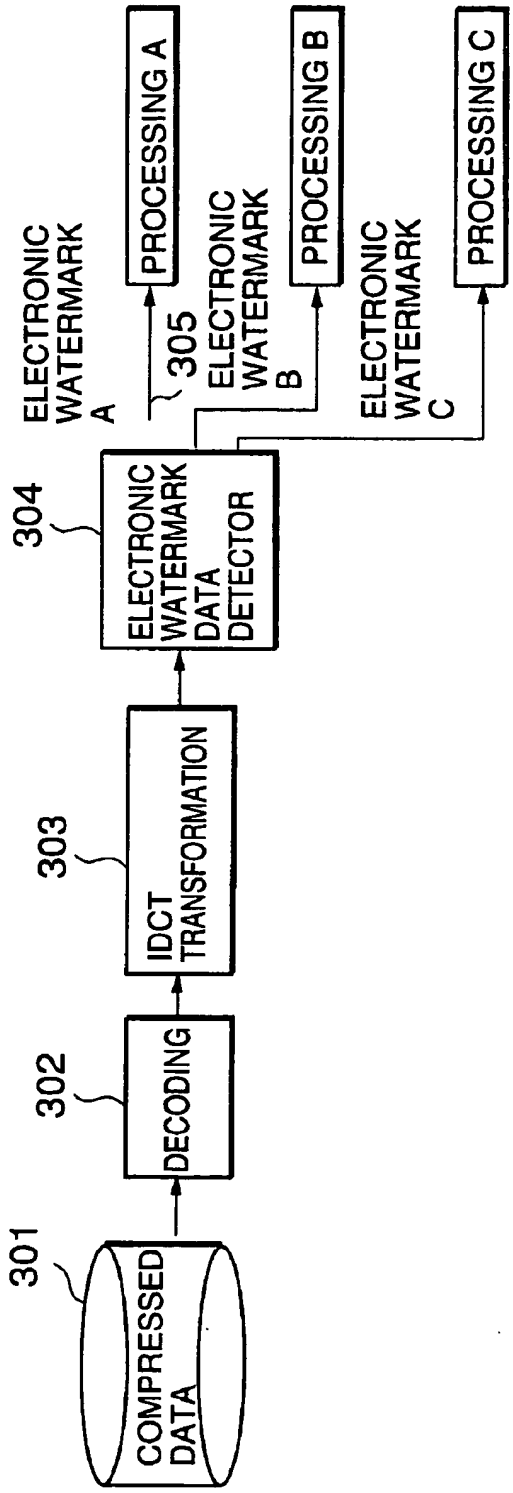

301
COMPRESSED DATA
302
DECODING
303
IDCT TRANSFORMATION
304
ELECTRONIC WATERMARK DATA DETECTOR
305
ELECTRONIC WATERMARK A
ELECTRONIC WATERMARK B
ELECTRONIC WATERMARK C
PROCESSING A
PROCESSING B
PROCESSING C

FIG.4

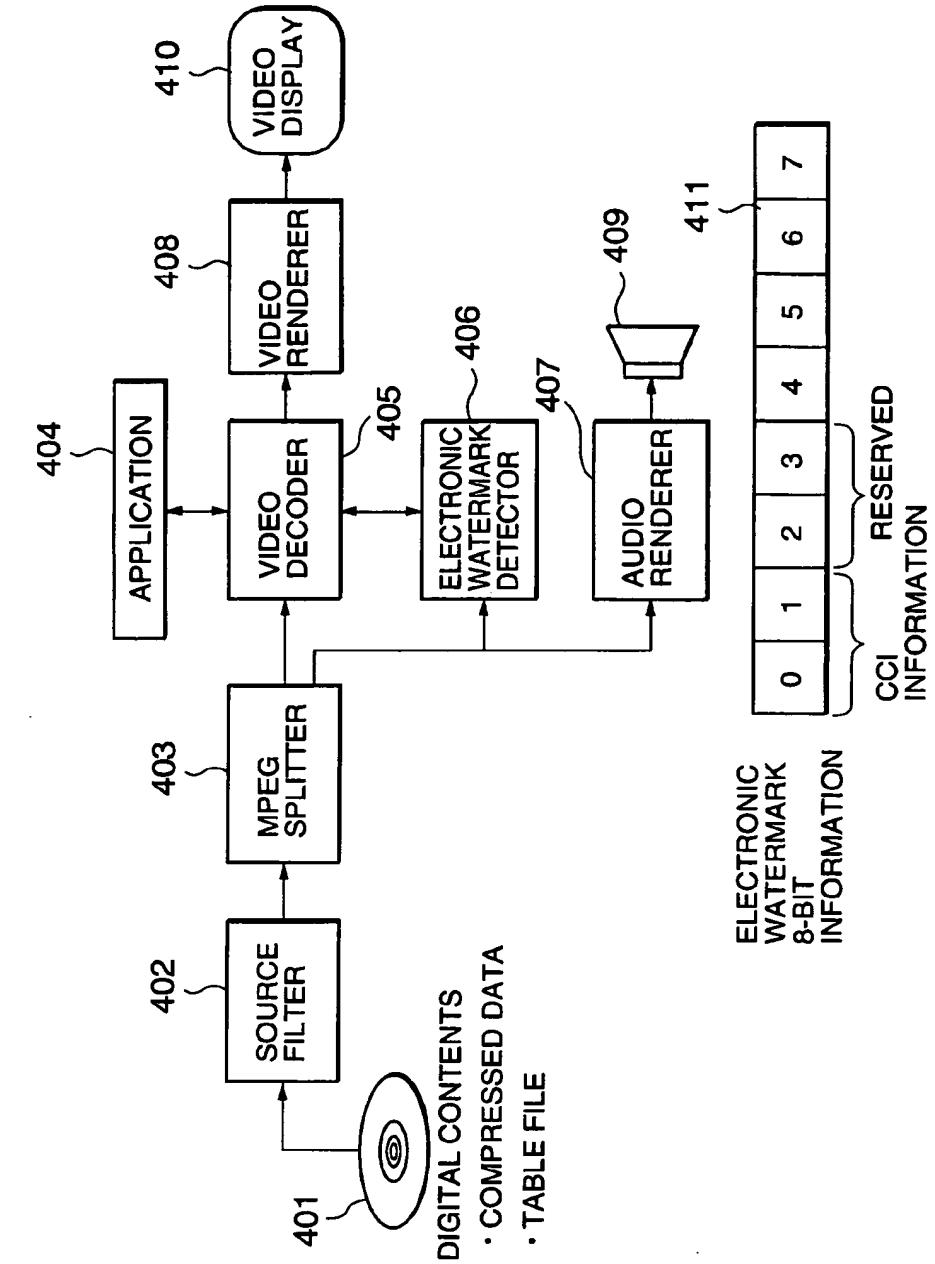
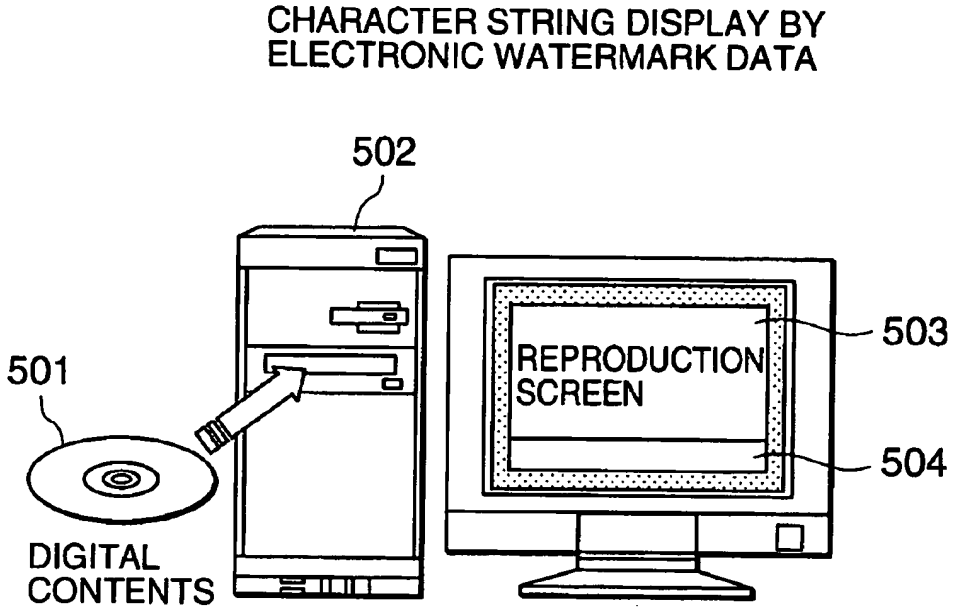

410
VIDEO DISPLAY
408
VIDEO RENDERER
404
APPLICATION
VIDEO DECODER
405
406
ELECTRONIC WATERMARK DETECTOR
407
409
AUDIO RENDERER
411
403
MPEG SPLITTER
402
SOURCE FILTER
401
DIGITAL CONTENTS
・COMPRESSED DATA
・TABLE FILE
0
1
2
3
4
5
6
7
CCI INFORMATION
RESERVED
ELECTRONIC WATERMARK 8-BIT INFORMATION

FIG.5

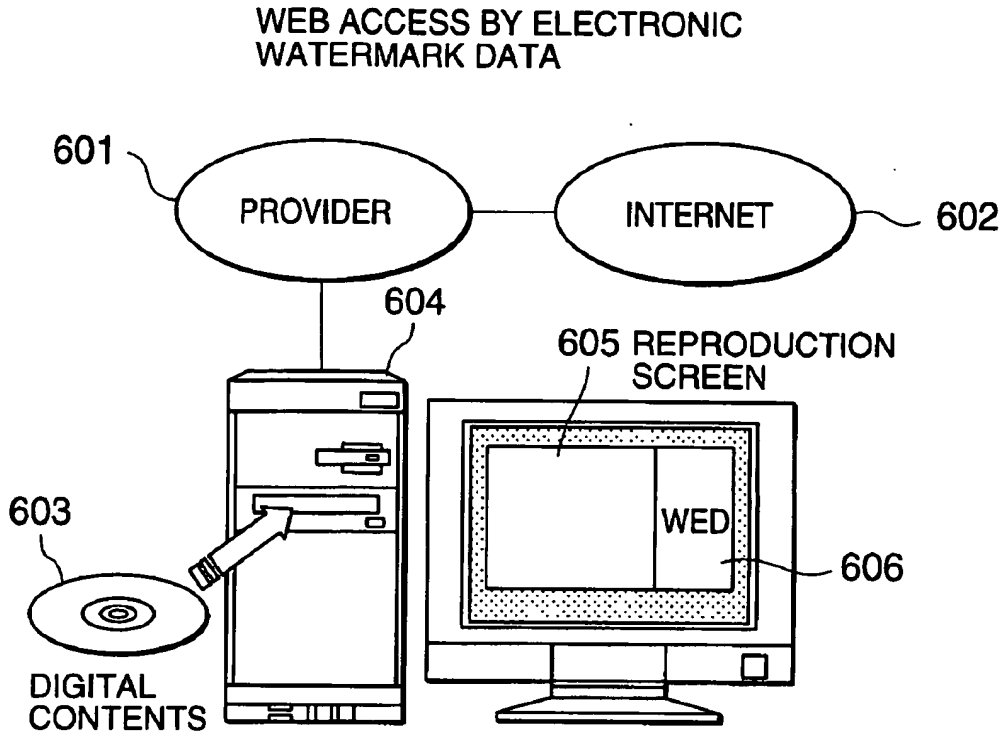


DEFINITION IN TABLE FILE

505

LOW-ORDER 4 BITS	DISPLAY CONTENTS
0000	DO NOT DISPLAY
0001	DISPLAY ADVERTISEMENT OF COMPANY A.
0010	DISPLAY ADVERTISEMENT OF COMPANY B.
⋮	⋮

FIG.6

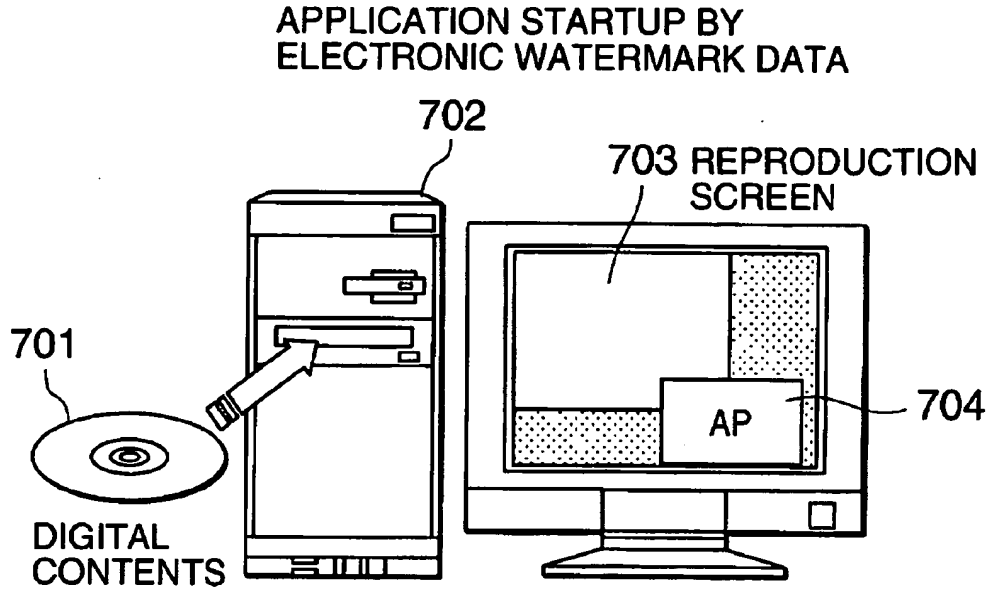


DEFINITION IN TABLE FILE

607

LOW-ORDER 4 BITS	DISPLAY CONTENTS
0000	DO NOT DISPLAY
0001	ACCESS http://abc
0010	ACCESS http://def
⋮	⋮

FIG.7



DEFINITION IN TABLE FILE

705

LOW-ORDER 4 BITS	DISPLAY CONTENTS
0000	DO NOT DISPLAY
0001	START APPLICATION A
0010	START APPLICATION B
⋮	⋮

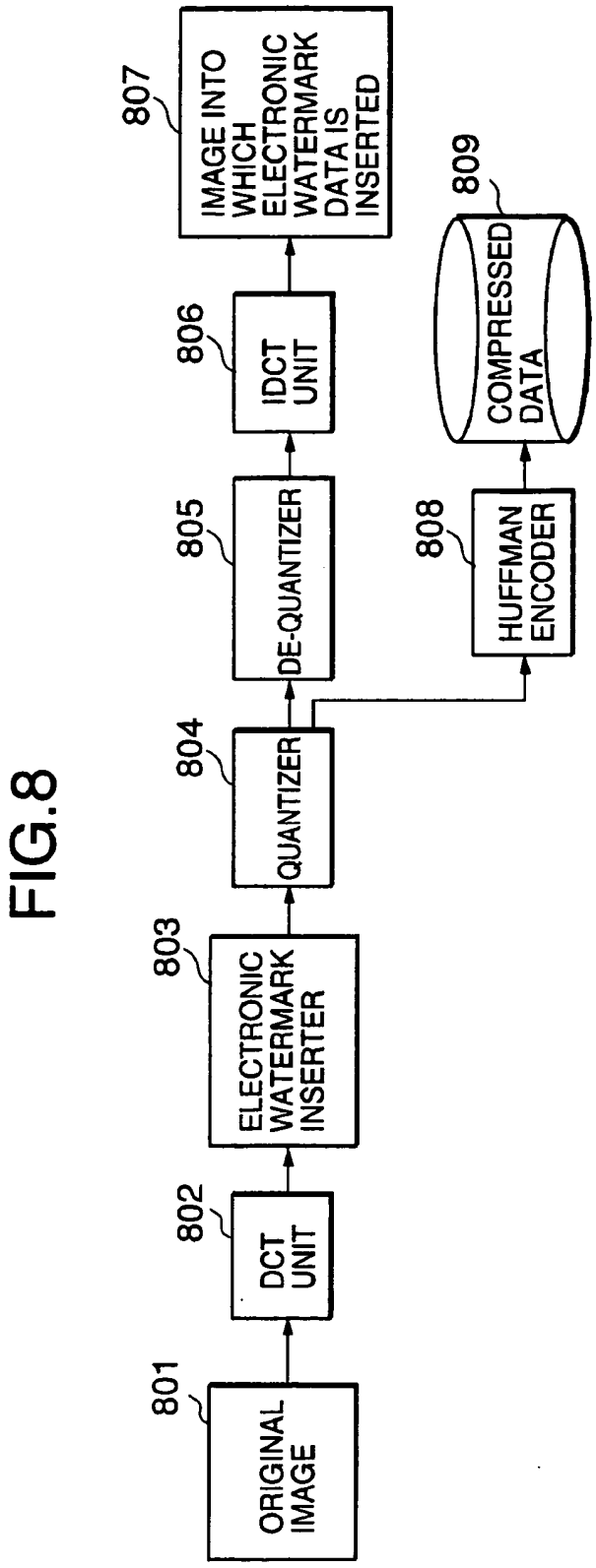

801
ORIGINAL IMAGE
802
DCT UNIT
803
ELECTRONIC WATERMARK INSERTER
804
QUANTIZER
805
DE-QUANTIZER
806
IDCT UNIT
807
IMAGE INTO WHICH ELECTRONIC WATERMARK DATA IS INSERTED
808
HUFFMAN ENCODER
809
COMPRESSED DATA

FIG.8

FIG.9

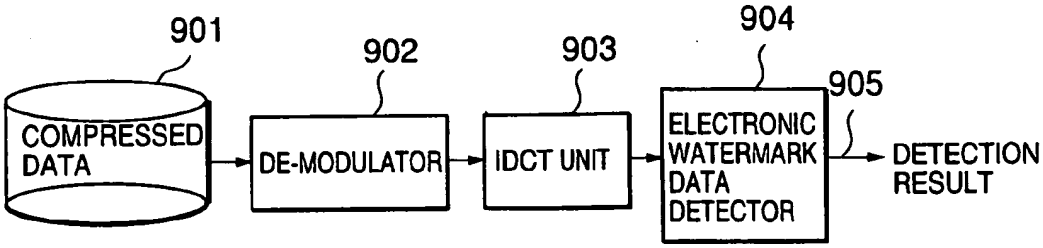
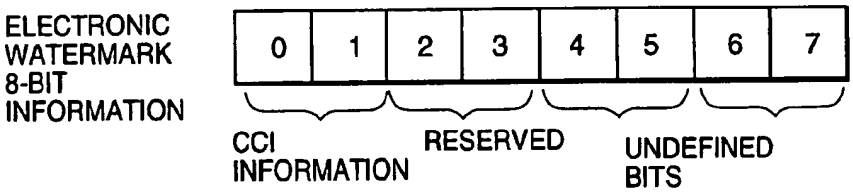

901
902
903
904
905
COMPRESSED DATA
DE-MODULATOR
IDCT UNIT
ELECTRONIC WATERMARK DATA DETECTOR
DETECTION RESULT

FIG.10


ELECTRONIC WATERMARK 8-BIT INFORMATION
0
1
2
3
4
5
6
7
CCI INFORMATION
RESERVED
UNDEFINED BITS

ELECTRONIC WATERMARK INSERTION DEVICE, DETECTION DEVICE, AND METHOD

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to a digital image, and more particularly to a device that inserts identification data, which has special information, into a digital image and a device that detects the identification data.

[0003] 2. Description of the Related Art

[0004] Recently, more and more data recorded on media is digitized. On the other hand, an illegal copy of data, brought by data digitization, has become a serious social problem. Electronic watermark (hereinafter called a watermark) insertion and detection technology, designed for preventing illegal copies, is now being studied for practical use. Watermark technology, a technology for embedding a sort of invisible ID information as a noise, is characterized in that embedded information that constantly coexists with contents cannot be erased or modified easily. Taking advantage of these characteristics, watermark insertion/detection technology prevents contents, such as video data, from being illegally copied.

[0005] As an example of electronic watermark technology, a method for embedding a watermark is proposed in which, after an image is frequency-converted, the watermark is embedded into an area where the frequency of video signal components is high. Because a watermark is embedded into a high-frequency component area in this method, the watermark will not be removed even if image processing, such as compression/decompression and filtering, is performed. The watermark embedded in this way is removed only when the original image is destroyed. In addition, arranging watermarks based on random numbers generated according to normal distribution avoids interference among watermarks, preventing image quality from being degraded.

[0006] This method embeds a watermark in the following steps. First, the original image is converted to frequency components using, for example, DCT (discrete cosine transform), and n data pieces, f(1), f(2), . . . f(n), each high in the frequency region, are selected. Then, watermarks, w(1), w(2), . . . ,w(n) are selected from those arranged according to normal distribution (average is 0, covariance is 1) and, for each i, the following calculation is executed.

$$F(i)=f(i)+\alpha\times|f(i)|\times w(i)$$

[0007] where, α is a scaling element.

[0008] Then, performing inverse DCT for F(i) gives an image in which a watermark is embedded.

[0009] This method detects a watermark in the following steps. This method requires that the original image f(i) and a watermark candidate w(i) (where, i=1, 2, . . . , n) be known.

[0010] First, an image with a watermark embedded is converted to frequency components using DCT. Let F(1), F(2), . . . , F(n) be the values of elements corresponding to f(1), f(2), . . . , f(n) each of which has a watermark embedded in the frequency region. A watermark W(i) is calculated and extracted using f(i) and F(i) as follows:

$$W(i)=(F(i)-f(i))/f(i)$$

[0011] Next, the statistical similarity between w(i) and W(i) is calculated using the inner product of the vector as follows:

$$C=W\ w/(WD\times wD)$$

[0012] where,

[0013] W=(W(1), W(2), . . . , W(n)),

[0014] w=(w(1), w(2), . . . , w(n)),

[0015] WD is the absolute value of vector W, wD is the absolute value of vector w, and is the inner product of the vector. When the statistical similarity C is a value equal to or larger than a specific value, it is judged that the watermark is embedded.

[0016] If a watermark is embedded in this method, the copyright holder of the original image may find the source of digital image data that is illegally copied. This method, which requires an original image, allows the copyright holder to detect a watermark only when he or she has the original image of image data which is thought to be copied illegally. However, on a terminal reproducer where the original image is not available, this method cannot be used to detect a watermark.

[0017] To solve this problem, a method improved for use on a terminal, especially for use in an MPEG system, is proposed. This method divides the original image into 8×8 pixel blocks and embeds and extracts a watermark into and from those blocks, one block at a time.

[0018] This method embeds a watermark in the following steps. First, let f(1), f(2), . . . , f(n) be the frequency components in the frequency region, arranged in AC frequency ascending order, for which discrete cosine transfer has been performed during MPEG compression. Then, watermarks w(1), w(2), . . . , w(n) are selected from those arranged according to normal distribution (average is 0, covariance is 1) and, for each i, the following calculation is executed,

$$F(i)=f(i)+\alpha\times avg(f(i))\times w(i)$$

[0019] where, α is a scaling element, and avg(f(i)) is a partial average of the absolute values in three points near f(i).

[0020] Then, processing that follows MPEG processing is performed using F(i) instead of f(i).

[0021] This method detects a watermark in the following steps. This method does not require the original image; only the watermark candidates w(i) (where, i=1, 2, . . . , n) need be known.

[0022] First, let F(1), F(2), . . . , F(n) be the frequency components in the frequency region, arranged in frequency ascending order, for which de-quantization has been performed during MPEG decompression. With the absolute value of the average of three points near F(i), that is, F(i−1), F(i), and F(i+1), as the partial average avg(F(i)), watermark W(i) is calculated from W(i)=F(i)/avg(F(i)) and, for each i, the total WF(i) of W(i) for one image is calculated.

[0023] Then, the statistical similarity of w(i) and WF(i) is calculated from C=WF w/(WFD×wD) using the inner product of the vector. When the statistical similarity C is a value equal to or larger than a specific value, it is judged that the watermark is embedded.

[0024] **FIG. 8** shows the configuration of a device that inserts an electronic watermark into MPEG-compressed image data. In the figure, numeral **802** indicates a DCT transformer that performs DCT (discrete cosine) transformation for an original image **801** and outputs DCT-transformed data, numeral **803** indicates a watermark inserter that puts watermark weighs on the DCT coefficients as described above, numeral **804** indicates a quantizer that quantizes the DCT coefficients into which a watermark is inserted, numeral **805** indicates a de-quantizer that de-quantizes quantized data, numeral **806** indicates an IDCT transformer that performs IDCT(inverse discrete cosine transform) for de-quantized data, numeral **807** indicates an image into which a watermark is inserted, numeral **808** indicates a Huffman encoder that performs Huffman coding to compress quantized data, and numeral **809** indicates data compressed through Huffman encoding. The device with this configuration inserts a watermark into the original image **801** and then provides general users with the compressed data **809** into which a watermark is inserted.

[0025] **FIG. 9** shows the configuration of a device that decodes the contents into which a watermark is inserted. In the figure, numeral **902** indicates a decoder that decodes compressed data **901** into which a watermark is inserted, numeral **903** indicates an IDCT transformer that performs IDCT for decoded data, and numeral **904** indicates a watermark detector that detects a watermark in data for which IDCT has been performed as described above. The device with this configuration detects a watermark inserted in the contents.

[0026] On the other hand, the configuration of a watermark is shown in **FIG. 10**. The high-order four bits of an eight-bit watermark contains information defined by the electronic watermark promotion organization. More specifically, the high-order two bits are defined as the CCI (copy protection) bits and bits **3-4** are reserved. The low-order four bits are undefined.

[0027] The use of only the high-order four bits are defined with the low-order four bits undefined as described above. How to use the remaining low-order four bits, reserved for future use, is a problem.

SUMMARY OF THE INVENTION

[0028] Object of the Invention

[0029] Accordingly, it is an object of the present invention to provide an electronic watermark insertion/detection device that efficiently uses the low-order four bits included but not defined in a watermark.

[0030] The present invention is characterized in that the undefined low-order four bits of an 8-bit watermark are defined for specific use and in that, at contents reproduction time, a predetermined operation is performed based on the information included in the low-order four bits. That is, as shown in **FIG. 1**, the device according to the present invention embeds a watermark **102** into an original image **101** to create an image in which the watermark is inserted. At contents reproduction time, the device detects the watermark included in the image and performs a predetermined operation based on the information stored in the low-order four bits of the detected watermark.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] **FIG. 1** is a block diagram showing the concept of the present invention.

[0032] **FIG. 2** is a block diagram showing an embodiment of an electronic watermark insertion device according to the present invention.

[0033] **FIG. 3** is a block diagram showing an embodiment of an electronic watermark detection device according to the present invention.

[0034] **FIG. 4** is a block diagram showing a system to which the electronic watermark detection device according to the present invention is applied.

[0035] **FIG. 5** is a block diagram showing the embodiment of the present invention.

[0036] **FIG. 6** is a block diagram showing the embodiment of the present invention.

[0037] **FIG. 7** is a block diagram showing the embodiment of the present invention.

[0038] **FIG. 8** is a block diagram showing a conventional electronic watermark insertion device.

[0039] **FIG. 9** is a block diagram showing a conventional electronic watermark detection device.

[0040] **FIG. 10** is a diagram showing the configuration of a conventional watermark.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0041] An embodiment of a watermark insertion/detection device according to the present invention will be described with reference to the attached drawings.

[0042] **FIG. 2** is a block diagram showing a watermark insertion device. This watermark insertion device differs from a prior-art device shown in **FIG. 8** in that predetermined information is saved in a table file **210**.

[0043] On the other hand, **FIG. 3** is a block diagram showing a watermark detection device. This watermark detection device differs from a prior-art device shown in **FIG. 8** in that, after the watermark is detected, processing is performed according to the detected watermark.

[0044] The operation of the present invention will be described below.

[0045] First, **FIG. 5** shows an example of character information displayed based on the low-order four bits of the watermark.

[0046] In the figure, numeral **501** indicates digital contents. The digital contents contain image data into which the watermark is inserted as well as a table file **505** defining the low-order four bits of the watermark. Numeral **502** indicates a computer that reproduces the digital contents and detects the watermark. Numeral **503** indicates a reproduction screen on which reproduced image data is displayed. Numeral **504** indicates a screen on which character information is displayed.

[0047] The computer **502** reads image data and the table file **505** from a recording medium on which digital contents are recorded. Next, the computer **502** reproduces the image

data and displays it on the reproduction screen **503**. In parallel with this operation, the computer **502** extracts a watermark from the image data that was read, compares the low-order four bits of the watermark with the information defined in the table file **505** and, based on the comparison result, performs a predetermined operation. For example, when the low-order four bits are [0000], the computer does not display data on the screen **504**. When the low-order four bits are [0001], the computer displays the advertisement of company A on the screen **504**. When the low-order four bits are [0010], the computer displays the advertisement of company B. Note that advertisement data that is displayed is pre-stored in the digital contents **501** or in the computer **502**.

[0048] Next, **FIG. 6** shows an example of how to access a web site on the Internet based on the low-order four bits on a watermark. In this example, the table file contains URLs used to access web sites on the Internet. Numeral **605** indicates a screen on which a reproduced image is displayed. Numeral **606** indicates a screen on which the web page of an accessed web site is displayed.

[0049] A personal computer **604** reproduces digital contents **603**. In parallel with this operation, the computer **603** extracts a watermark, compares the low-order four bits of the watermark with the information defined in the table file **607** and, based on the comparison result, performs a predetermined operation. For example, when the low-order four bits of the watermark are [0000], the computer does not display data on the screen **606**. When the low-order four bits are [0001], the computer automatically accesses [http://abc] and displays the contents of the web page on the screen **606**. When the low-order four bits are [0010], the computer accesses [http://def] and displays the contents of the web page on the screen **606**.

[0050] Next, **FIG. 7** shows an example of starting an application program based on the low-order four bits of the watermark. In this example, the table file contains the names of files used for executing application programs. Numeral **703** indicates a window in which a reproduced image is displayed, and numeral **704** indicates a window in which an application program is displayed.

[0051] A personal computer **702** reproduces digital contents **701**. In parallel with this operation, the computer **702** extracts a watermark, compares the low-order four bits of the watermark with the information described in the table file **705** and, based on the comparison result, performs a predetermined operation. For example, when the low-order four bits of the watermark are [0000], the computer does not display data in the window **704**. When the low-order four bits are [0001], the computer automatically starts application program A and displays the result in the window **704**. When the low-order four bits are [0010], the computer starts application program B and displays the result in the window **704**.

[0052] Although the table file is used in the three examples described above, ASCII-coded data may be inserted directly into an image as a watermark instead of using the table file. In this case, when the watermark is detected, a predetermined operation is executed. That is, character data coded, for example, in ASCII code may be inserted directly into the low-order four bits of a watermark. When the watermark is detected, the character data is displayed, a web site is accessed automatically, or an application program is started.

[0053] Finally, a system to which the electronic watermark detection device according to the present invention is applied will be described. Compressed data generated when a watermark is inserted and a table file are stored in a medium such as a DVD. They are distributed to an end user as digital contents **401**. In general, the digital contents **401** are reproduced on a reproduction device such as a DVD player or a personal computer. In the description below, an example of reproduction on a personal computer will be described. A source filter **402** reads data from the digital contents **401**. The data, once read, is split into video data and audio data by an MPEG splitter **403**. Video data, generated by the splitting of the MPEG splitter **403**, is decoded by a video decoder **405** and is output to a video renderer **408**. At this time, the video decoder **405** outputs data, required for detecting a watermark, to a watermark detector **406**. The watermark detector **406** detects a watermark based on the data and passes the detected result to an application **404** via the video decoder. The detected watermark is 8-bit information **411**. The application **404** references the table file pre-stored in the digital contents and performs a predetermined operation as described above. A video renderer **408** performs processing for displaying decoded video data and displays the video.

[0054] Although the watermark is 8 bits in length and the device uses the low-order four bits of the eight bits in the above description, the watermark may be n bits in length (for example, 16 bits, 32 bits, etc.) and the device may use m bits (m=<n). That is, the number of bits of a watermark does not matter.

[0055] The device according to the present invention allows a watermark to be used not only for copy protection but also for other purposes. Therefore, the device finds more applications in the system without having to add major modifications to the conventional system.

What is claimed is:

1. A device that embeds an electronic watermark into an original image, comprising:

a circuit that performs discrete cosine transform (DCT) for the original image to output DCT coefficients;

a circuit that embeds the watermark into the DCT coefficients, the watermark containing in a part thereof an instruction to an electronic watermark detection device;

a circuit that quantizes the DCT coefficients into which the watermark is embedded; and

a circuit that variable-length encodes the quantized DCT coefficients.

2. The device according to claim 1 wherein the electronic watermark is eight-bit data and the instruction is four-bit data.

3. The device according to claim 1 or 2 wherein the instruction displays characters.

4. The device according to claim 1 or 2 wherein the instruction accesses a web site on the Internet.

5. The device according to claim 1 or 2 wherein the instruction starts an application program.

6. A device that detects an electronic watermark embedded in an original image, comprising:

a circuit that decodes compressed image data in which the watermark is embedded;

a circuit that performs inverse discrete cosine transform (IDCT) for the decoded data;

a circuit that detects electronic watermark data embedded in the data for which IDCT has been performed; and

a circuit that performs a predetermined processing according to an instruction included in a part of the electronic watermark.

7. The device according to claim 6 wherein the electronic watermark is eight-bit data and the instruction is four-bit data.

8. The device according to claim 6 or 7 wherein characters are displayed according to the instruction.

9. The device according to claim 6 or 7 wherein a web site on the Internet is accessed according to the instruction.

10. The device according to claim 6 or 7 wherein an application program is started according to the instruction.

11. A method for embedding an electronic watermark into an original image, comprising the steps of:

performing discrete cosine transform (DCT) for the original image to output DCT coefficients;

embedding the watermark into the DCT coefficients, the watermark containing in a part thereof an instruction to an electronic watermark detection device;

quantizing the DCT coefficients into which the watermark is embedded; and

variable-length encoding the quantized DCT coefficients.

12. The method for inserting a watermark according to claim 11 wherein the electronic watermark is eight-bit data and the instruction is four-bit data.

13. The method according to claim 11 or 12 wherein the instruction displays characters.

14. The method according to claim 11 or 12 wherein the instruction accesses a web site on the Internet.

15. The method according to claim 11 or 12 wherein the instruction starts an application program.

16. A method for detecting an electronic watermark embedded in an original image, comprising the steps of:

decoding compressed image data in which the watermark is embedded;

performing inverse discrete cosine transform (IDCT) for the decoded data;

detecting electronic watermark data embedded in the data for which IDCT has been performed; and

performing a predetermined processing according to an instruction included in a part of the electronic watermark.

17. The method according to claim 16 wherein the electronic watermark is eight-bit data and the instruction is four-bit data.

18. The method according to claim 16 or 17 wherein characters are displayed according to the instruction.

19. The method according to claim 16 or 17 wherein a web site on the Internet is accessed according to the instruction.

20. The method according to claim 16 or 17 wherein an application program is started according to the instruction.

21. A computer readable recording medium storing therein a program for embedding an electronic watermark into an original image, said program causing a computer to:

perform discrete cosine transform (DCT) for the original image to output DCT coefficients;

embed the watermark into the DCT coefficients, the watermark containing in a part thereof an instruction to an electronic watermark detection device;

quantize the DCT coefficients into which the watermark is embedded; and

variable-length encode the quantized DCT coefficients.

22. A computer-readable recording medium storing therein a program for detecting an electronic watermark embedded in an original image, said program causing a computer to:

decode compressed image data in which the watermark is embedded;

perform inverse discrete cosine transform (IDCT) for the decoded data;

detect electronic watermark data embedded in the data for which IDCT has been performed; and

perform a predetermined processing according to an instruction included in a part of the electronic watermark.

* * * * *